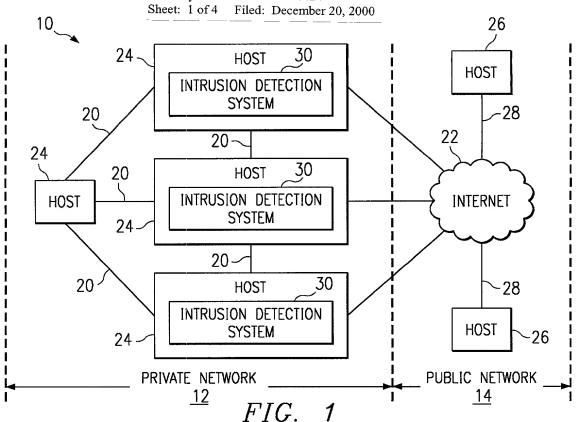Method and System for Maintaining
Network Activity Data for Intrusion
Detection
Inventor: Wiley, et al.
Attorney's Docket: 062891.0424
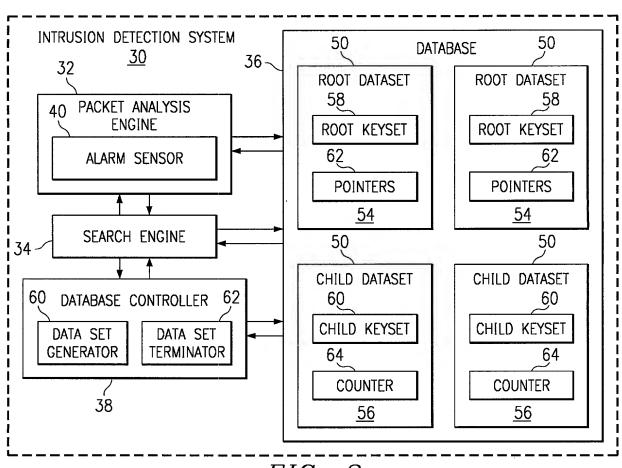Sheet: 1 of 4   Filed: December 20, 2000

FIG. 1

FIG. 2

Method and System for Maintaining Network Activity Data for Intrusion Detection
Inventor: Wiley, et al.
Attorney's Docket: 062891.0424
Sheet: 2 of 4   Filed: December 20, 2000

FIG. 3A

ROOT KEYSET — 54

DstIp	DstPort	ScrIp	ScrPort	ACTIVITY COUNTER	1st POINTER	2nd POINTER	3rd POINTER	4th POINTER	TERMINATION STATUS
120	122	124	126	104	106	108	110	112	114

102

FIG. 3B

CHILD KEYSET — 56

DstIp	DstPort	ScrIp	ScrPort	ACTIVITY COUNTER	ROOT COUNTER
150	152	154	156	144	146

142

FIG. 4

A a B b
A x B x
x x B b
A x x b

B b A a
B x A x
x x A a
B x x a

180

Method and System for Maintaining
Network Activity Data for Intrusion
Detection
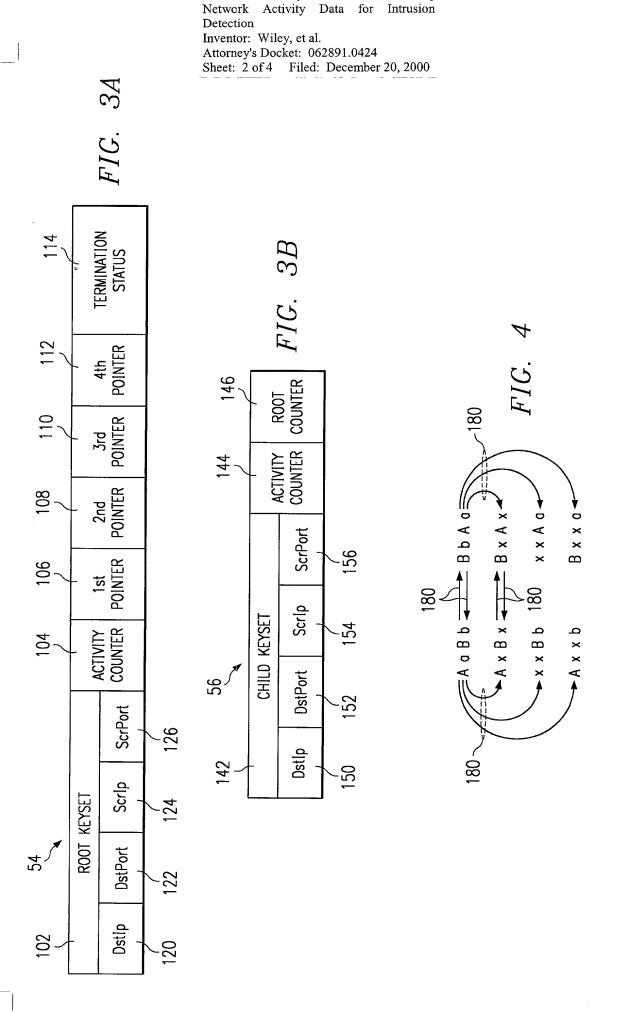Inventor: Wiley, et al.
Attorney's Docket: 062891.0424
Sheet: 3 of 4   Filed: December 20, 2000

FIG. 5

START

200 — IDENTIFY TRAFFIC SIGNATURE FOR INTRUSION DETECTION PROCESSING

202 — SEARCH NETWORK ACTIVITY DATA FOR NEXT DATASET CORRESPONDING TO SIGNATURE

204 — ROOT DATASET EXIST? —YES→

NO

206 — GENERATE ROOT DATASET

208 — SEARCH NETWORK ACTIVITY DATA FOR SIBLING DATASET

210 — SIBLING DATASET EXIST? —YES→

NO

212 — GENERATE SIBLING DATASET

214 — SEARCH NETWORK ACTIVITY DATA FOR DATASETS

216 — ALL CHILD DATASETS EXIST? —YES→

NO

218 — GENERATE ABSENT CHILD DATASETS

220 — ASSOCIATE ROOT, SIBLING AND CHILD DATASETS

222 — IDENTIFY ROOT DATASET

224 — IDENTIFY SIBLING AND CHILD DATASETS FROM ROOT DATASET

226 — RETRIEVE DATA FROM ROOT, CHILD, SIBLING AND KEY DATASETS FOR SIGNATURE

228 — COMPARE DATA TO INTRUSION DETECTION LIMITS THRESHOLDS

230 — ATTACK UNDERWAY? NO / YES

232 — ALARM

END

Method and System for Maintaining
Network Activity Data for Intrusion
Detection
Inventor: Wiley, et al.
Attorney's Docket: 062891.0424
Sheet: 4 of 4   Filed: December 20, 2000

(START)

250 — IDENTIFY EMPTY
ROOT DATASET

252 — ROOT DATASET RECORDS
RECORD FOR
TERMINATION STATUS

254 — DETERMINE TERMINATION
STATUS OF SIBLING DATASET

256 — SIBLING
READY FOR
TERMINATION?   NO

YES

258 — TERMINATE SIBLING

260 — TERMINATE ALL CHILD
DATASETS WITH NO ROOT
DATASETS

262 — TERMINATE ROOT DATASET

(END)

FIG. 6